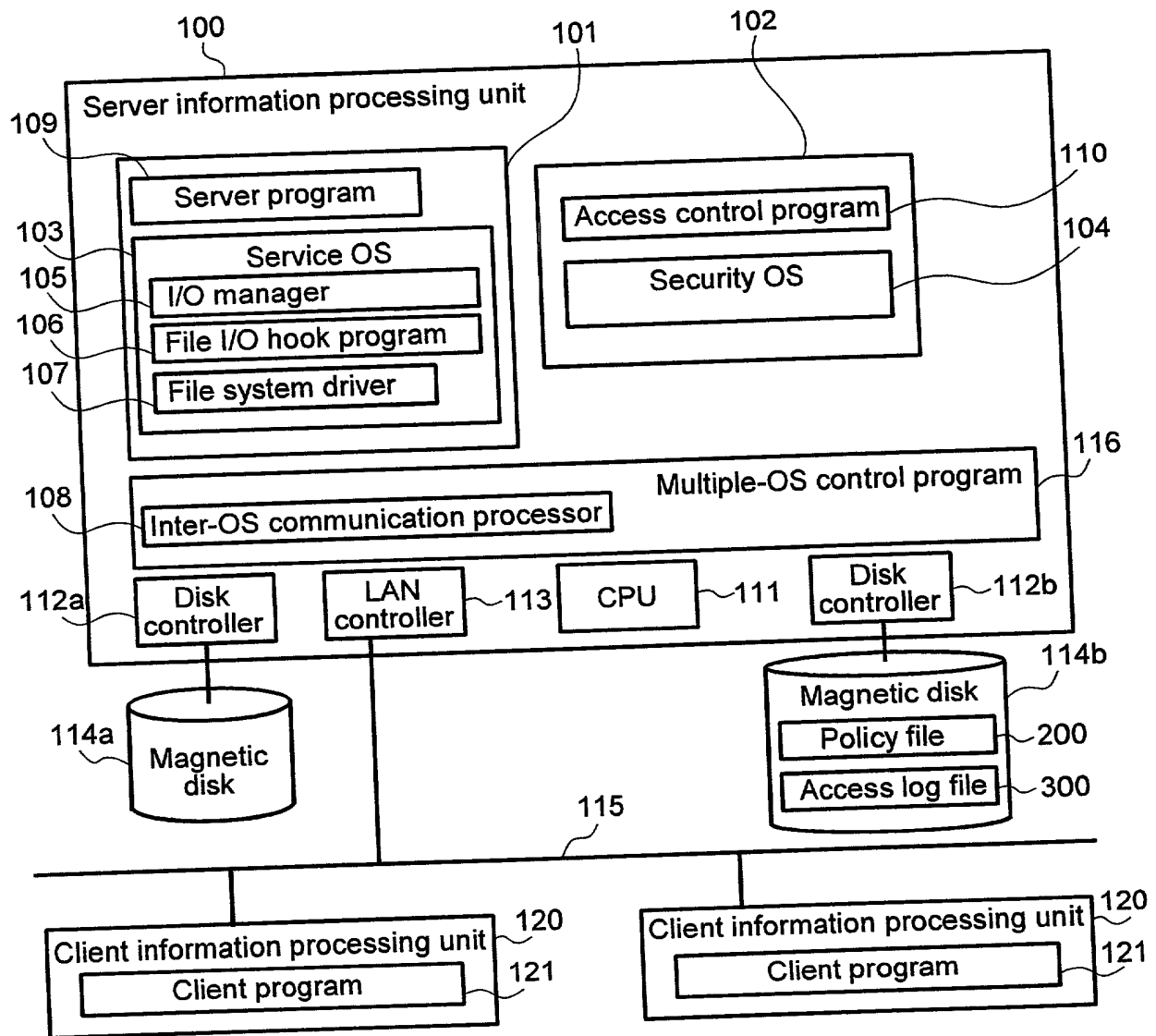


FIG.1



100: Server information processing unit

120: Client information processing unit

101: Memory under the control of service OS

102: Memory under the control of security OS

[illegible]

200: Policy file

Atty Docket No. 16869P016300

Applicant: Masato Arai, et al.

Title: Access Control System

Sheet 3 of 16

FIG. 3

| 300 | | 301 | | 302 | | 303 | | 304 | | 305 | |
|---------------------|--|-----------------------|--|-------------|--|-------------------------|--|-----------|--|-----|--|
| Date/time | | Object name | | Access type | | Subject name | | User name | | | |
| 1999.07.28 15:32:46 | | D: ¥ DOC ¥ SECRET.TXT | | Write | | C: ¥ prog ¥ wwwsrv.exe | | u_0023 | | | |
| 1999.07.27 09:15:10 | | D: ¥ DOC ¥ SECRET.TXT | | Delete | | C: ¥ prog ¥ wwwsrv.exe | | u_0023 | | | |
| 1999.07.25 16:02:55 | | D: ¥ SYS ¥ CONFIG ¥ | | Write | | C: ¥ prog ¥ txtedit.exe | | intruder | | | |
| 1999.07.25 14:44:28 | | D: ¥ SYS ¥ CONFIG ¥ | | Delete | | C: ¥ prog ¥ fileman.exe | | intruder | | | |
| 1999.07.25 14:42:59 | | D: ¥ LOG ¥ LOG.TXT | | Read | | C: ¥ prog ¥ txtedit.exe | | user007 | | | |
| 1999.07.16 10:29:31 | | D: ¥ LOG ¥ LOG.TXT | | Delete | | C: ¥ prog ¥ fileman.exe | | user007 | | | |

300: Access log file

Atty Docket No. 16869P016300

Applicant: Masato Arai, et al.

Title: Access Control System

Sheet 4 of 17

FIG. 4

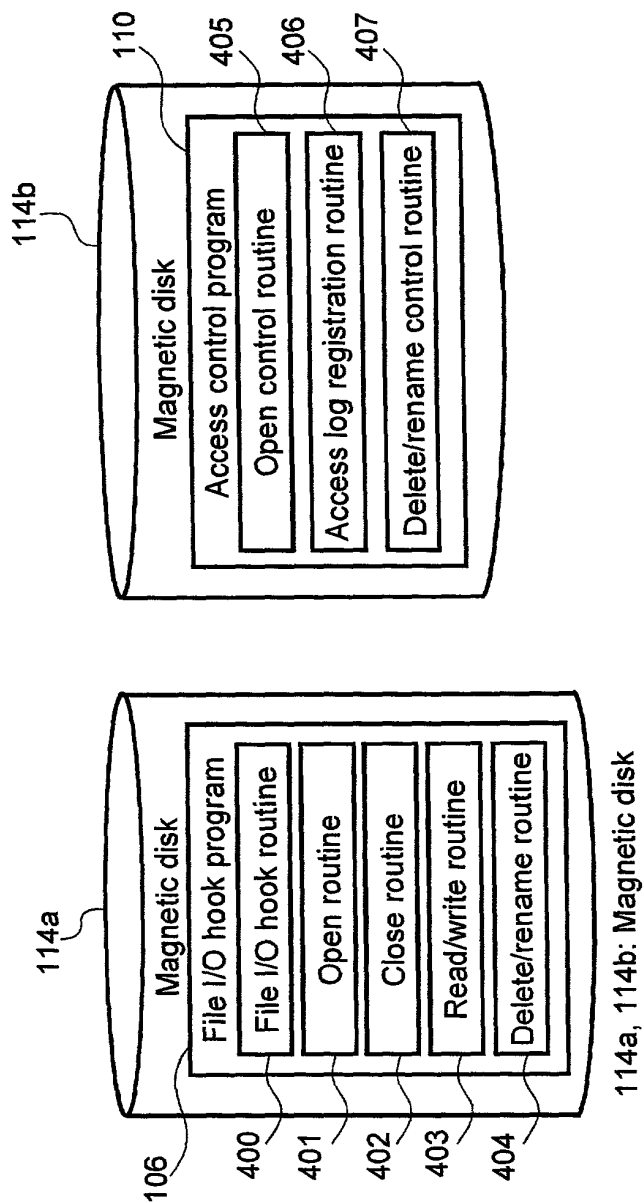
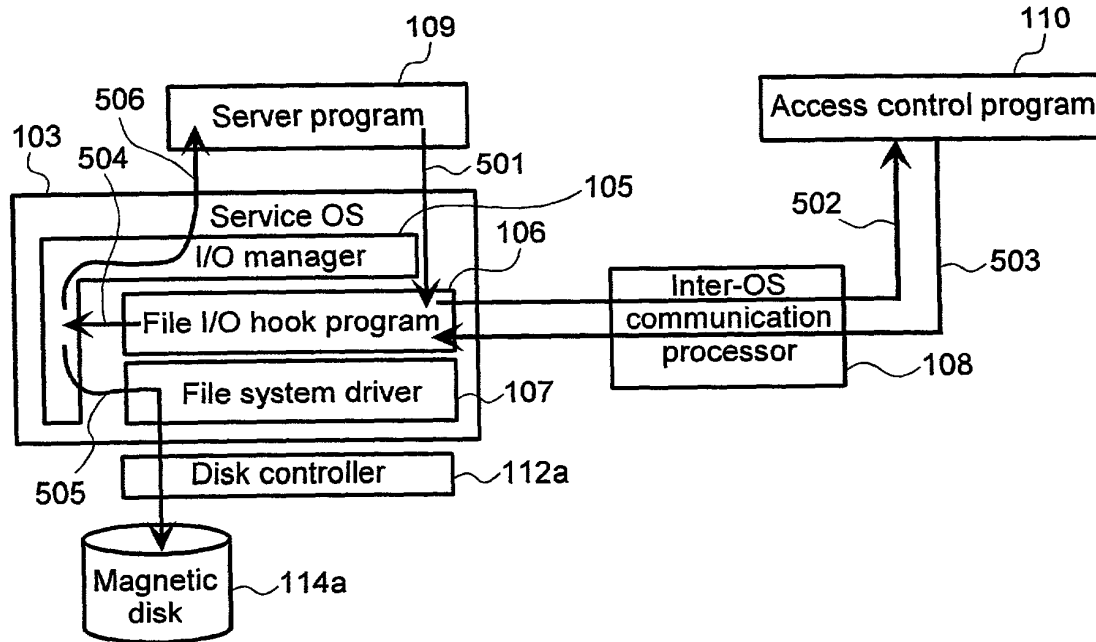
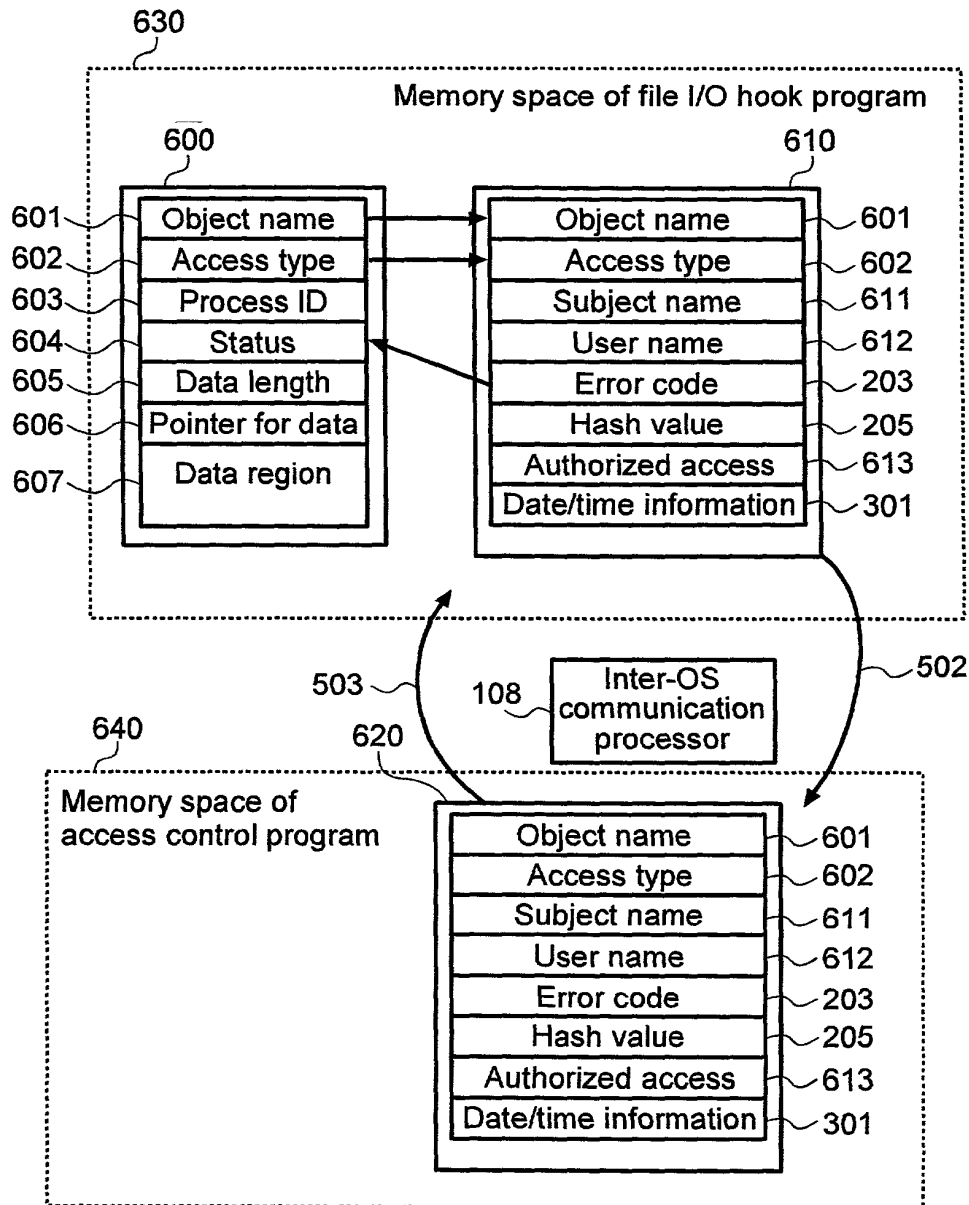


FIG.5



501~506: Communication routes

FIG.6

600: I/O packet

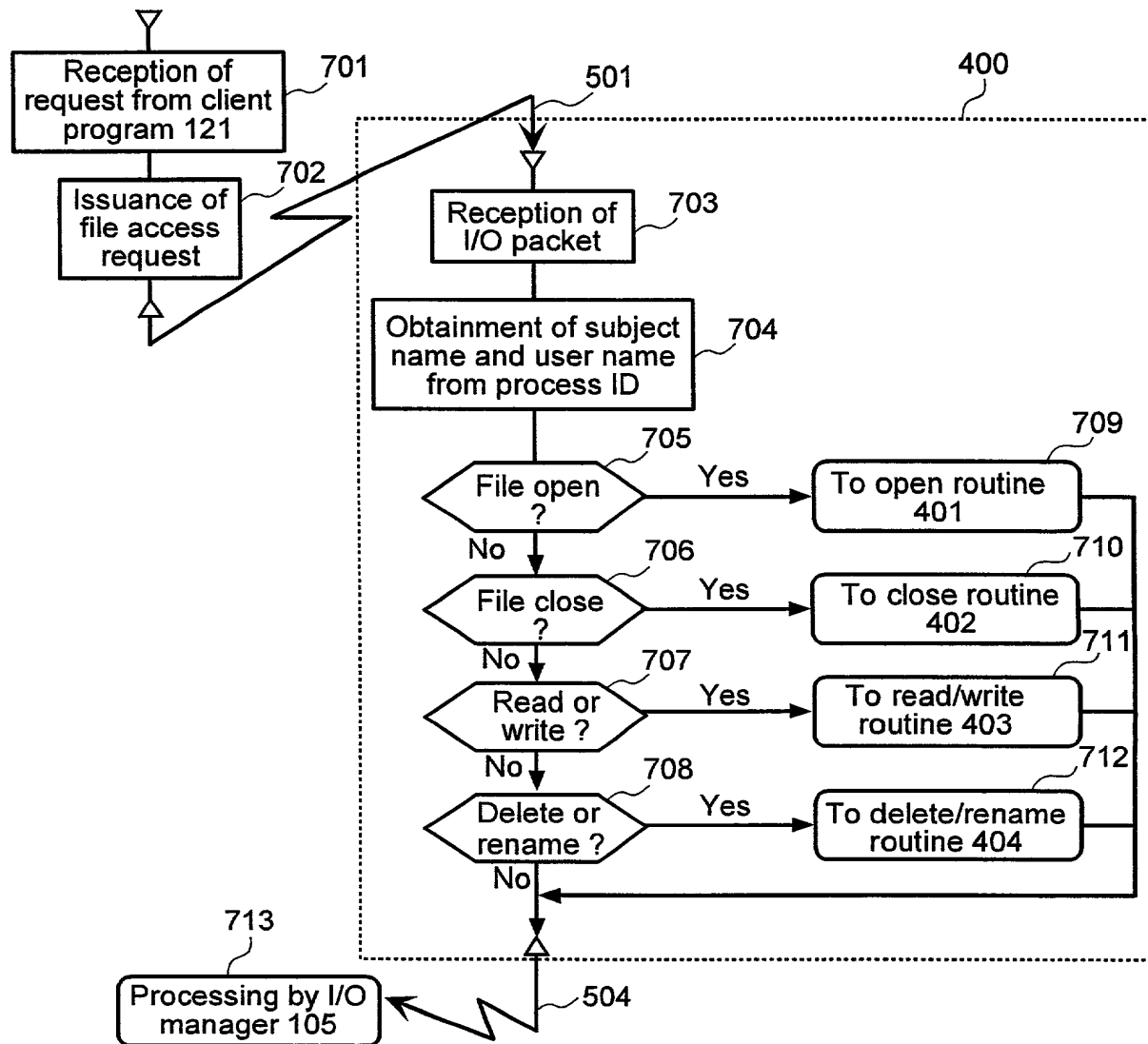
610: Request packet

620: Response packet

630: Memory space of file I/O hook program

640: Memory space of access control program

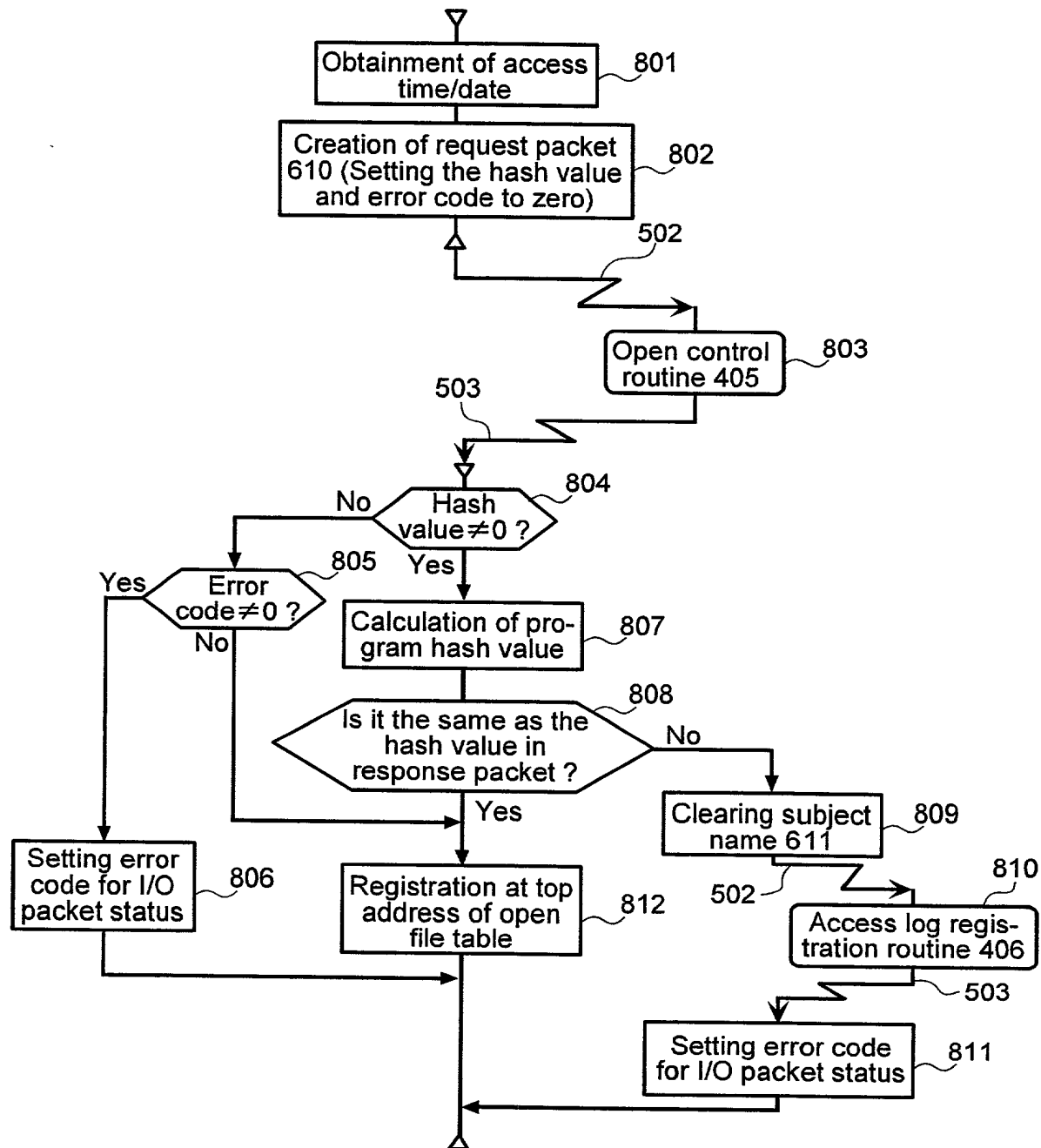
FIG.7



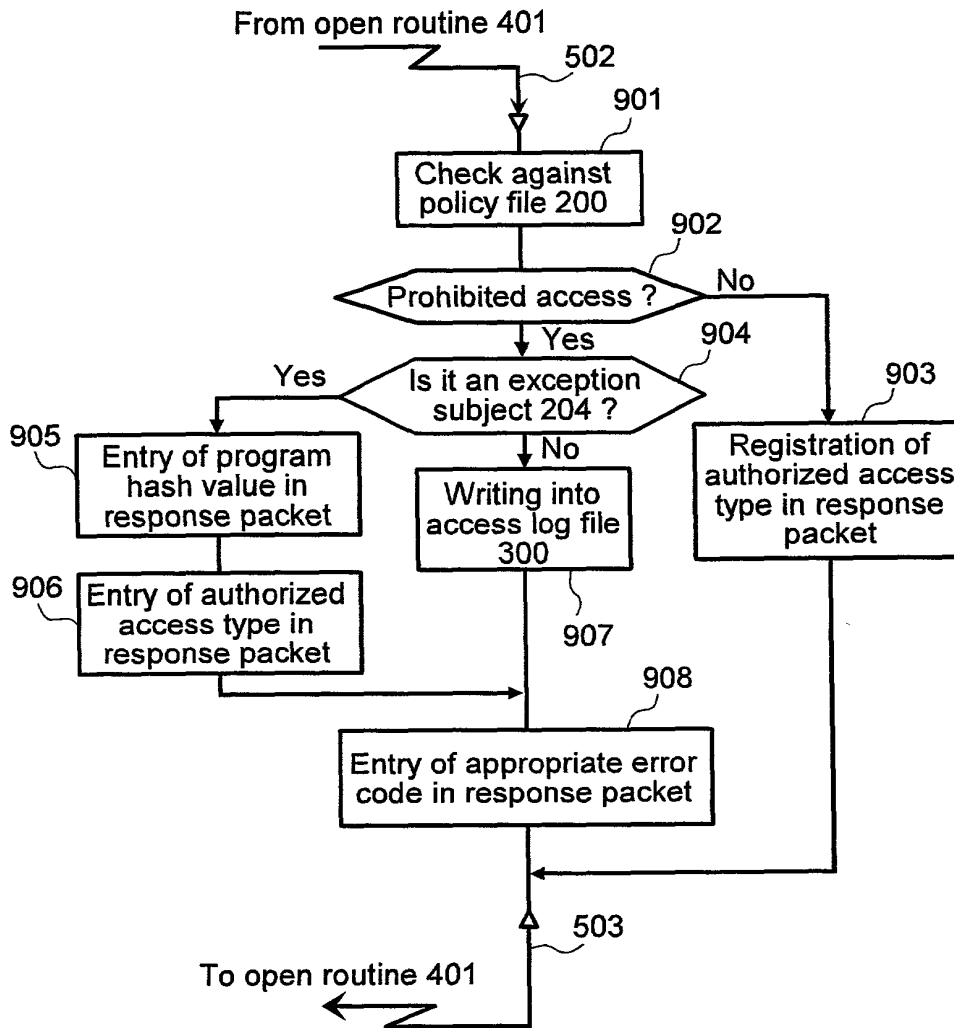
701~702: An outline of the processing sequence for the server program 109

703~712: Processing sequence for the file I/O hook routine 400

FIG.8

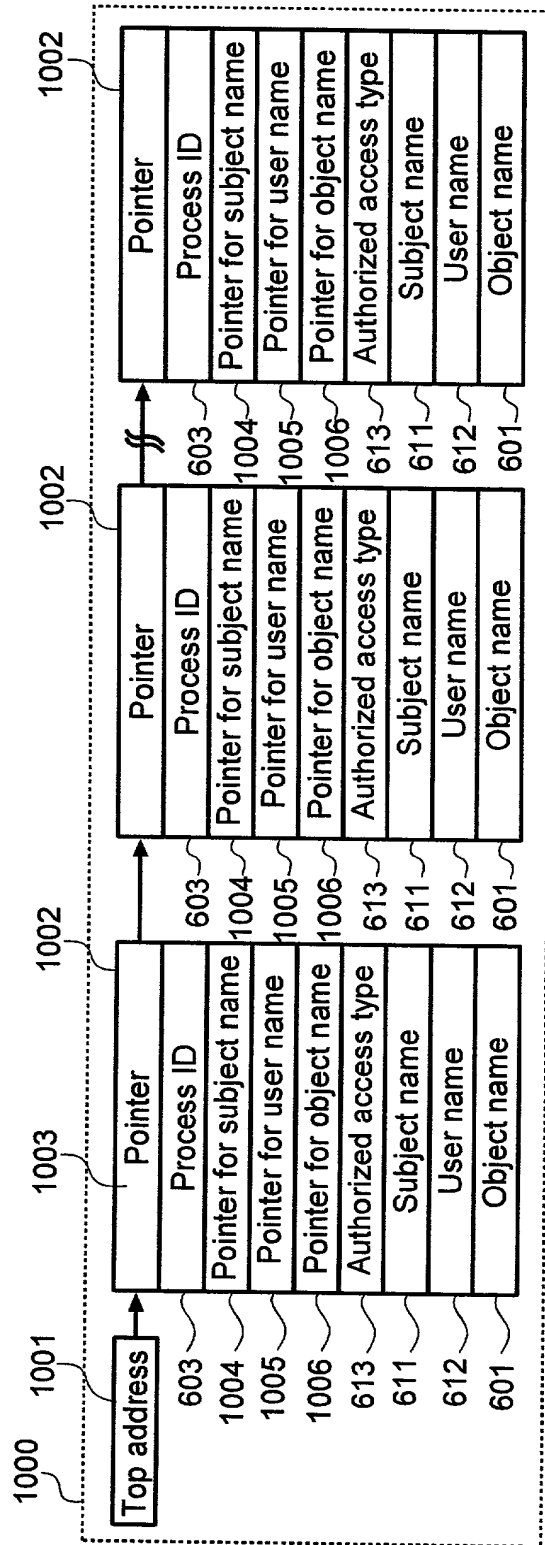


801~812: Processing sequence for the open routine

FIG.9

901~908: Processing sequence for the open control routine 405

FIG.10

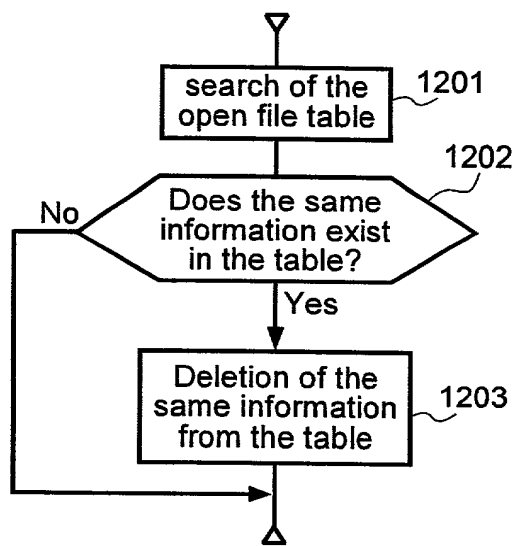


1000: Open file table

1002: Open file structured data

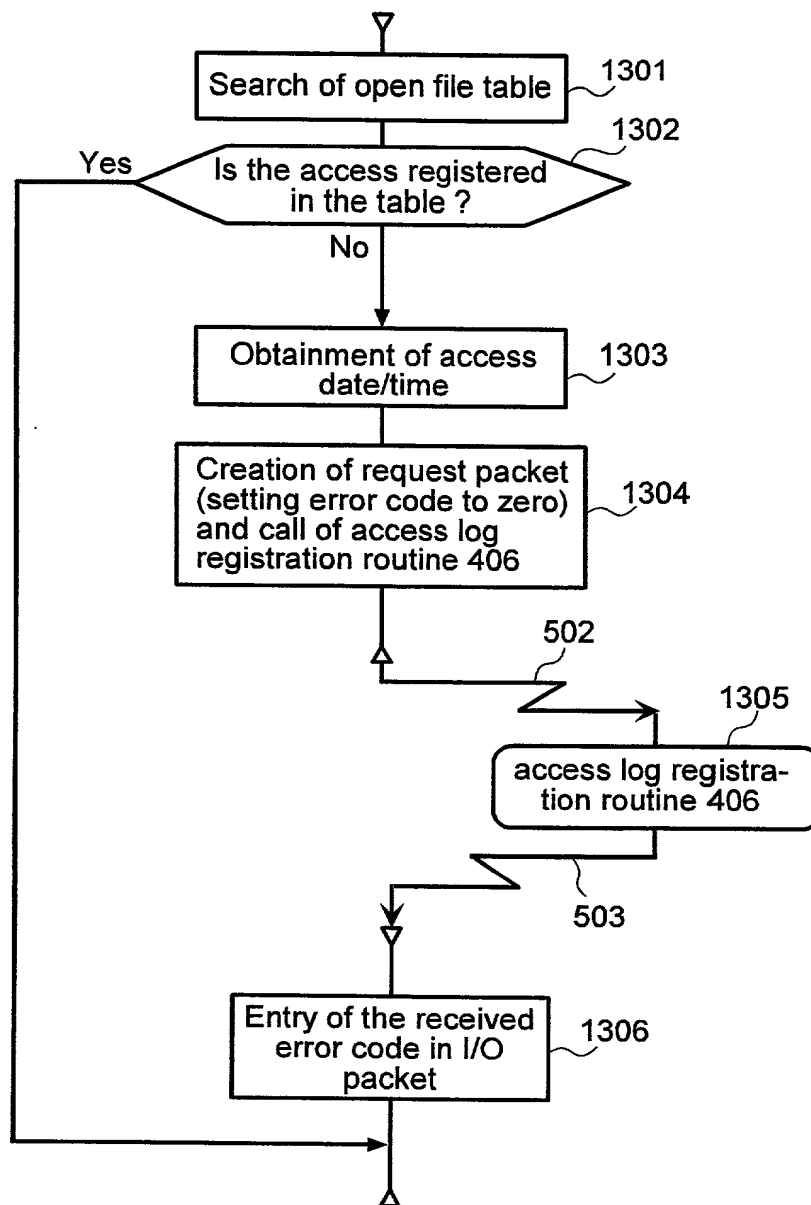
FIG. 11

| | | | | | |
|------------|----------------------|-----------|--------------------|------------------------|-----|
| 1000 | 603 | 611 | 612 | 601 | 613 |
| Process ID | Subject name | User name | Object name | Authorized access type | |
| 0022 | c:\prog\wwwserv.exe | inet | D:\HOME\SALES.HTML | Read | |
| 0043 | c:\prog\wordedit.exe | sec_admin | D:\DOC\SECRET.TXT | Read/Write | |
| 0067 | c:\prog\viewer.exe | tarou | D:\DOC\IDEA.TXT | Read | |
| 0092 | c:\prog\mantool.exe | sys_admin | D:\SYS\CONFIG\PORT | Read/Write | |
| 0113 | c:\prog\vcck.exe | system | D:\DOC\SHEET.DOC | Read | |
| 0218 | c:\prog\audit.exe | root | D:\LOG\LOG.TXT | Read/Write | |

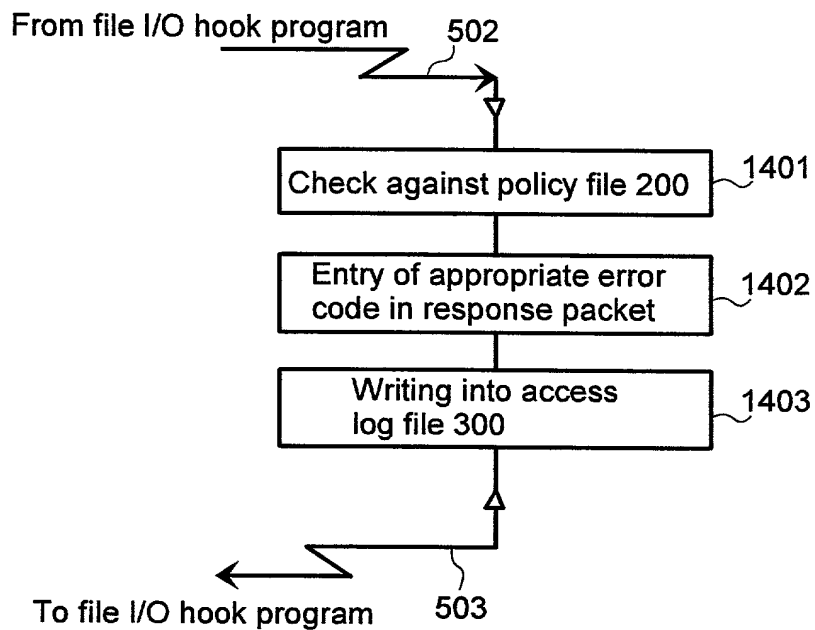
FIG.12

1201~1203: Processing sequence for the close routine 402

FIG.13

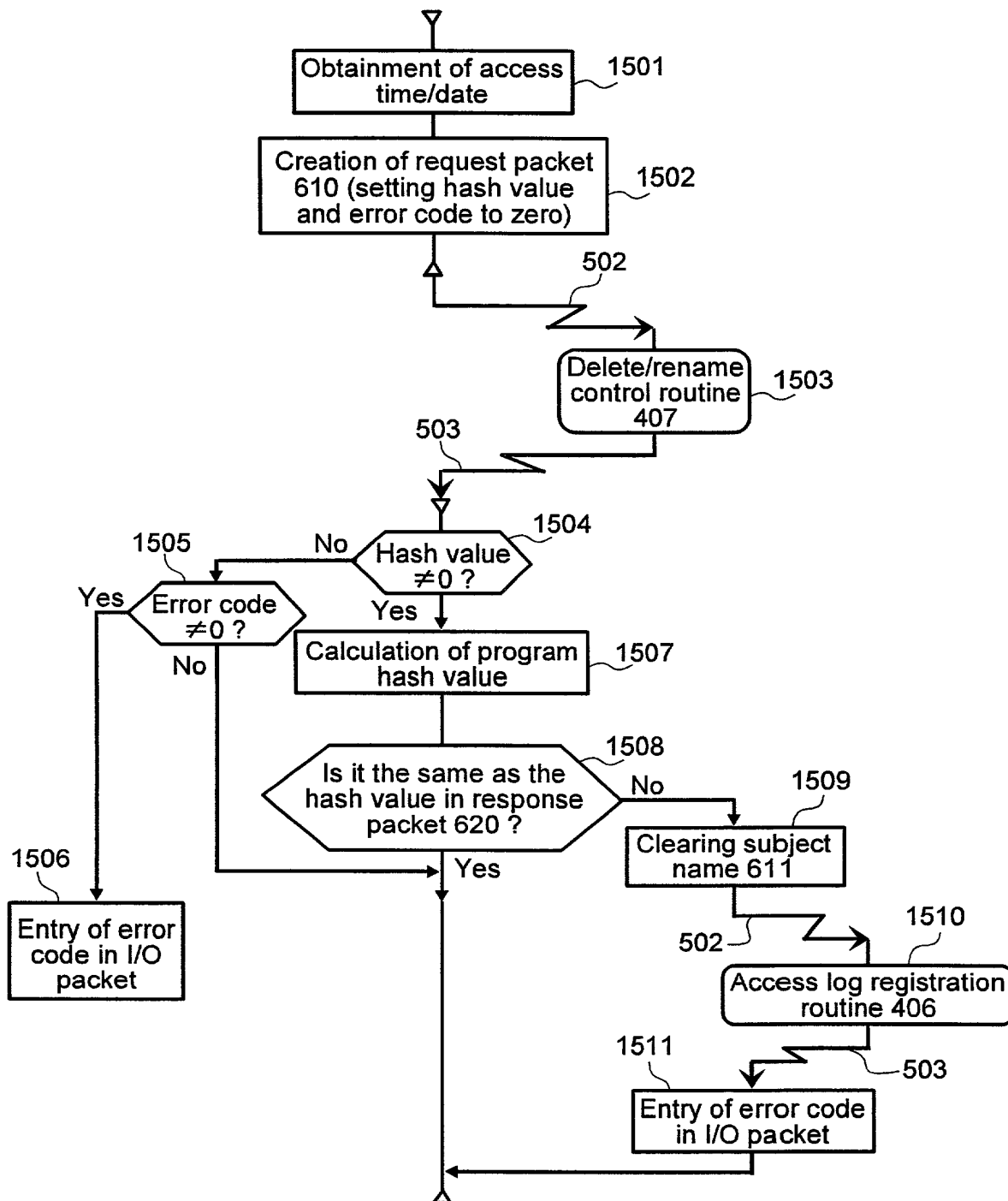


1301~1306: Processing sequence for the read/write routine 403

FIG.14

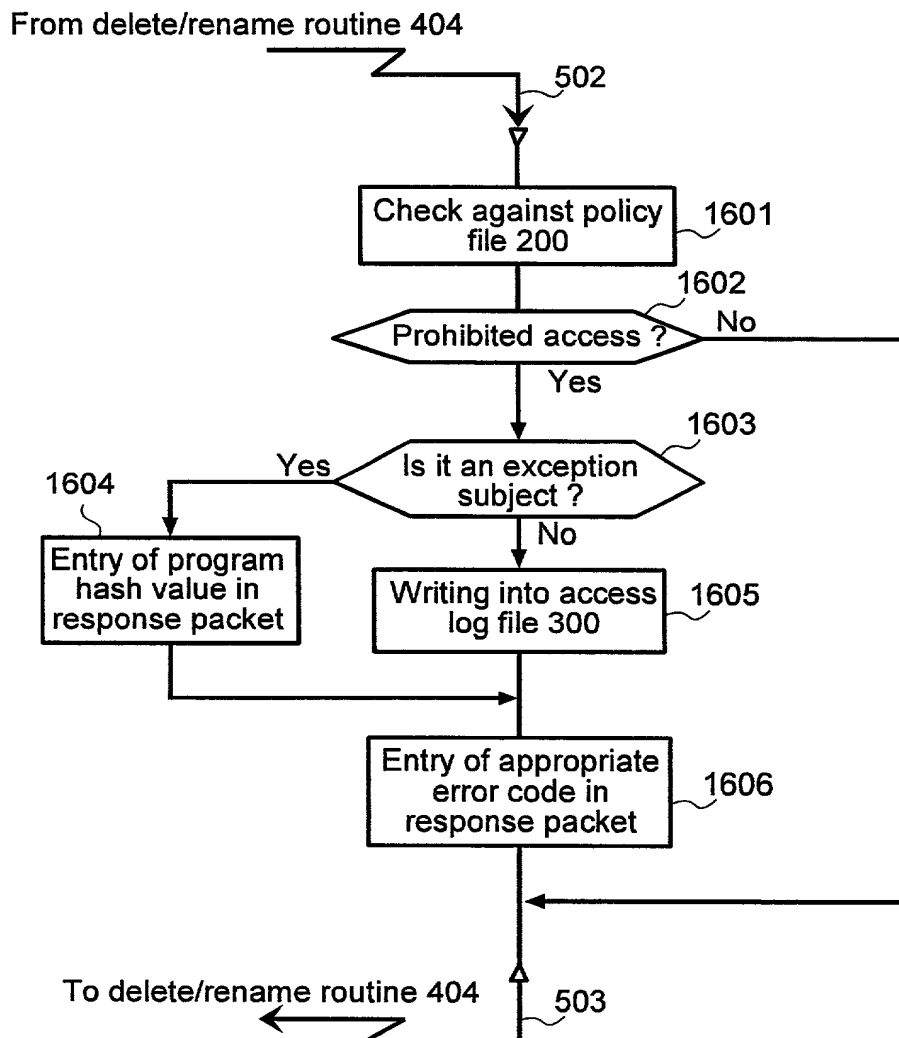
1401~1403: Processing sequence for the access log registration routine 406

FIG.15



1501~1511: Processing sequence for the delete/rename routine 404

FIG.16



1601~1605: Processing sequence for the delete/rename control routine 407

FIG.17

